(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 719 045 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
26.06.1996 Bulletin 1996/26

(51) Int. Cl.[6]: **H04N 7/167**

(21) Application number: **95119605.4**

(22) Date of filing: **13.12.1995**

(84) Designated Contracting States:
DE FR GB

(30) Priority: **13.12.1994 JP 309292/94**

(71) Applicant: **MITSUBISHI CORPORATION**
Chiyoda-ku Tokyo 100 (JP)

(72) Inventor: **Saito, Makato**
Tama-shi, Tokyo (JP)

(74) Representative: **Neidl-Stippler, Cornelia, Dr.**
Rauchstrasse 2
D-81679 München (DE)

(54) Crypt key system for broadcast programmes

(57) The invention relates to a crypt key system applicable to a television system, a database system or an electronic commercial transaction system or the like. This system consists of a broadcasting station 11, a database 12, a receiving apparatus 14, a data communication apparatus 15 and a user terminal 18. As a crypt key system, a secret-key cryptosystem, a public-key cryptosystem, and a digital signature system are used. The keys used in the system are either encrypted or remain uncrypted to be supplied by broadcasting. The present invention is effective in the prevention of an unjustified use of the database system, managing copyrights, and in a pay-per-view system and a video-on-demand system. Further, the present invention is effective in realizing an electronic market which uses an electronic data information system.

EP 0 719 045 A2

Printed by Rank Xerox (UK) Business Services
2.12.4/3.4

Description

Background of the Invention

Field of the Invention

The present invention relates to a crypt key system that is used in a commercial trade or the like which uses a television system, a database system or an electronic data interchange.

Prior Art

In information oriented society of today, in addition to a normal terrestrial broadcasting, satellite broadcasting which is referred to as a broadcasting satellites (BS) and communication satellites (CS) or cable TV broadcasting which is referred to as CATV (cable television) using coaxial cables or optical cables is getting prevalent.

In a satellite broadcasting or CATV broadcasting which distributes several tens of channels at the same time, scrambled channels of such as films, sport events, and music which cannot be viewed through a comprehensive contracts are provided in addition to unscrambled general channels. In order to view these channels, it is necessary to subscribe to descramble the channels; however, normal subscription period is about one- month unit, and it is impossible to view through temporary contracts.

The inventor of the present invention proposed in the Japanese Patent Application Laid-Open No. 6-46419 and the Japanese Patent Application Laid-Open No.6-141004 a system in which users obtain a viewing permit key from a charging center via a communication line and charged, and descrambles programs scrambled each by respectively different scramble pattern, using the viewing permit key to view the programs; proposed in the Japanese Patent Application Laid-Open No. 6-132916 an apparatus for the operation.

In these system and apparatus, those who wish to use scrambled programs request for viewing to the charging center via a communication line by using a communication apparatus. The charging center transmits the viewing permit key to the communication apparatus corresponding to the request for viewing while charging and collecting a fee.

Users, on receiving the viewing permit key with the communication apparatus, transmits the viewing permit key via direct means connecting the communication apparatus and the receiving apparatus or via indirect means such as flexible disks or the like. The receiving apparatus to which the viewing permit key is transmitted descrambles the programs with the viewing permit key and then, the users use the programs.

Japanese Patent Application Laid-Open No. 6-132916 describes a system and an apparatus for sell and rent of a tape or a disk on which a plurality of data scrambled with a different scramble pattern respectively are recorded to supply the viewing permit key with IC cards or the like and use a specific data.

In addition, in these days of information- oriented society, a database system has been propagated for mutually using data which are kept independently by each computer by constituting a computer communication network by LAN (local area network), WAN (wide area network), and Inter-Net system mutually connecting these networks.

In the meantime, a technology has been developed for reducing the information amount by compressing a television moving picture signal which could not be digitized because of a huge amount of information as a result of digitization, to enable practical digitalization. So far, H.261 standard for video conference, JPEG (joint photographic image coding experts group) standard for static pictures, MPEG 1 (moving picture image coding experts group 1) standard for storing pictures and MPEG 2 corresponding to the present telecast and the high- definition telecast from the television broadcasting are prepared.

The digitization technology using these picture compression technology is used for the television broadcasting or the video picture recording. In addition, even television moving picture data which could not be dealt with before can be dealt with now. Then, the "multimedia system" which deals with various data dealt with by the computer and the digitized television moving picture data has been focused as a future technology.

This multimedia system is also incorporated in the data communication and can be used as one data on the database.

While the scope of usage of the database is expanded, the method for charging for the data usage on the database, and the method for dealing with copyright problems generated by copying, transmitting other than direct usage of data, and also the secondary exploitation right problem generated as a result of data edition have become important problems.

To safely deal with charging and copyrights process, it is required that the data cannot be used by users other than authorized users, and data encryption is the best means for it.

In addition, an electronic market system has been investigated for converting information in various kinds of transaction which has been carried out by paper documents so far, into an electronic data to execute electronic transaction by using the electronic data interchange for transmitting and receiving data by the data communication technology. In addition, an investigation is also made on the possibility of carrying out an electronical settlement on the electronic commercial transaction system

In the commercial transactions, the reliability on the transaction details is required and the security in the settlement is required. Consequently, in the electronic commercial transaction system and electronic settlement system in which such reliability and security are

demanded, it is required that the data is encrypted so that the data will not be falsified or used unjustifiedly.

In these television system, database system or electronic commercial transaction system or the like, the data is encrypted and thus a crypt key is required for decrypting the encrypted data to us. And the crypt key must be given to data users; however, the processing is very troublesome because security and reliability are demanded.

In the structure of the present invention, data cryptology acts an important part. In the beginning, a general explanation will be made on the data cryptology.

In the data cryptology, the case in which the plaintext data M is encrypted by using a crypt key K to obtain a cryptogram data C is represented:

$$C=E(K, M),$$

and the case in which the cryptogram data C is decrypted by using the crypt key K to obtain the plaintext data M is represented:

$$M=D(K, C).$$

As a typical method for the data cryptography technology, there are a secret-key cryptosystem and a public-key cryptosystem. The secret-key cryptosystem is a cryptosystem in which same secret key Ks is commonly used in encryption and decryption:

$$Cmks=E(Ks, M)$$

$$M=D(Ks, Cmks).$$

The public- key cryptosystem is a cryptosystem in which a key for encryption and a key for decryption are used as crypt keys, and the key for encryption is laid open but the key for decryption is not open. The key for encryption is referred to as a public key Kb while the key for decryption is referred to as a private-key Kv. To use this cryptosystem,an information sender encrypts the plaintext data M by the pubic-key Kb of a receiver

$$Cmkb=E(Kb, M),$$

and the receiver receives the data and decrypts it by a private-key Kv to obtain the plaintext data M

$$M=D(Kv, Cmkb).$$

In this public-key cryptosystem, cryptanalysis is very difficult.

As an application of the data cryptography technology, digital signature is performed as an electronic data authentication means to ensure the reliability of the data.

The digital signature is used a secret-key or a public-key. Generally, the public-key is used in the digital signature.

In the digital signature which is carried out by using the public-key, the signer obtains a digital signature by encrypting a document m to which the document M is compressed with hash algorithm, using the private-key Kv of the signer:

$$Smkv=E(Kv, m)$$

and transmits the original document M or the compressed document m and the digital signature Smkv to the receiver.

The receiver decrypts the digital signature Smkv by using the public-key Kb of the signer

$$m'=D(Kb, Smkv).$$

When m'=m is established, it is recognized that the signature is correct.

As a method for providing these crypt keys to users, the inventor of the present invention proposed an invention entitled "crypt key system" in the prior Japanese Patent Application No. 6-70643.

In the generally practiced crypt key system, the crypt key is provided only to users while the crypt key is provided to persons other than the users in the crypt key system of this prior invention.

Fig. 1 shows the structure of the crypt key system proposed in the Japanese Patent Application No. 6-70643.

This system comprises a broadcasting station 1 for multiplex boadcasting such as BS,CS, terrestrial broadcasting or FM or the like or data broadcasting, a database 2, a charging center 3, a receiving apparatus 4, data communication apparatus 5 and a user's terminal 8.

The broadcasting station 1 and the database 2, and the database 2 and the charging center 3 are connected to each other via a communication line such as a dedicated line or the like or flexible disc or the like. The database 2 and the data communication apparatus 5 are connected by a communication line 7 such as a communication line or CATV line.

The broadcasting station 1 and the receiving apparatus 4 are connected with the broadcasting radio wave 6. The receiving apparatus 4 and the user terminal apparatus 8, and the data communication apparatus 5 and the user terminal 8 are connected with a direct means such as a connection cable or an indirect means such as a flexible disc.

In Fig. 1, what is shown with a solid line is a path of information which is not encrypted. What is shown with a broken line is a path of data which is encrypted.

In this system, the database 2 preliminarily supplies a permit key Kp (hereinafter referred to as a "permit key") including the crypt key Kd which is different from one data to another to the broadcasting station 1. The permit key Kp is explained in such a manner that the permit key Kp constitutes the crypt key Kd only for better understanding.

In some cases, the crypt key Kd is supplied without being encrypted, and in other cases, it is encrypted by using the common crypt key K0

Ckdk0=E (K0, Kd),

and is supplied as an encrypted crypt key Ckdk0.

In the case where the crypt key Kd is encrypted and supplied, a common crypt key K0 for decrypting the encrypted crypt key Ckdk0 is supplied to users. This common crypt key K0 is supplied when users register with the database, or it is supplied to the users together with the encrypted data Cmkd when the encrypted data Cmkd is transmitted.

(a) In the case where the crypt key is not encrypted:

In this crypt key system, the broadcasting station 1 broadcasts the crypt key Kd supplied from the database 2, by using the radio wave 6.

The receiving apparatus 4 supplies the received crypt key Kd to the user terminal 8 so that the user terminal 8 stores the received crypt key Kd in a recording medium such as a semiconductor memory, a flexible disc, a hard disc or the like.

The users who wish to use the data request for the use of the data M to the database 2 via the communication line 7 by using the data communication apparatus 5.

The database 2 which has received the request for use of the data M encrypts the data M by the crypt key Kd which is a permit key Kp

Cmkd=E (Kd, M),

and transmits the encrypted data Cmkd to the data communication apparatus 5 of users via the communication line 7 and charges with the charging center 3.

The data communication apparatus 5 supplies the received encrypted data Cmkd to the user terminal 8 while the user terminal 8 decrypts the encrypted data Cmkd by the crypt key Kd which is stored in the recording medium

M=D (Kd, Cmkd).

(b) In the case where the crypt key is encrypted and the common crypt key is preliminarily distributed to users:

In this crypt key system, when users register to use the database, the common crypt key K0 is supplied to users with the recording medium such as ROM or flexible disc and the supplied common crypt key K0 is stored in the user terminal 8.

The database 2 encrypts the crypt key Kd by using the common crypt key K0

Ckdk0=E (K0, Kd),

and supplies encrypted crypt key Ckdk0 to the broadcasting station 1.

The broadcasting station 1 broadcasts the received encrypted crypt key Ckdk0 supplied from database 2 by using the radio wave 6.

The receiving apparatus 4 supplies the received encrypted crypt key Ckdk0 to the user terminal 8 which decrypts the encrypted crypt key Ckdk0 in the beginning by the preliminarily stored common crypt key K0

Kd=D (K0, Ckdk0),

and stores the decrypted crypt key Kd in the recording medium such as a semiconductor memory, a flexible disc or a hard disc.

Users who wish to use the data requests for the use of the data M to the database 2 via the communication line 7 by using the data communication apparatus 5.

The database 2 which receives the request for the data usage encrypts the data M which is demanded for usage encrypts data M by the crypt key Kd

Cmkd=E (Kd, M),

and transmits it to the data communication apparatus 5 via the communication line 7 and chargess with the charging center 3.

The data communication apparatus 5 supplies the received encrypted data Cmkd to the user terminal 8 which decrypts the encrypted data Cmkd by the stored crypt key Kd

M=D (Kd, Cmkd).

(c) In the case where the crypt key is encrypted and the common crypt key is distributed to the user together with the encrypted data:

In this crypt key system, the database 2 encrypt the crypt key Kd by the common crypt key K0

Ckdk0=E (K0, Kd)

and supplies it to the broadcasting station 1.

The broadcasting station 1 broadcasts the encrypted crypt key Ckdk0 which has been supplied from the database 2, by using the radio wave 6.

The receiving apparatus 4 supplies the received encrypted crypt key Ckdk0 to the user terminal 8. The user terminal 8 stores the encrypted crypt key Ckdk0 in recording medium such as a semiconductor memory, a flexible disc, or a hard disc or the like.

Users who wish to use the data request for the use of the data M to the database 2 via the communication line 7 by using the data communication apparatus 5.

The database 2 which receives the request for the data usage encrypts the data M which is demanded for use by the crypt key Kd

Cmkd=E (Kd, M),

and transmits it to the data communication apparatus 5 via the communication line 7 together with the common crypt key K0 and charges with the charging center 3.

The data communication apparatus 5 supplies the received encrypted data Cmkd and the common crypt key K0 to the user terminal 8. The user terminal 8 decrypts the encrypted crypt key Ckdk0 which has been stored in the recording medium by the common crypt key K0

$$Kd=D(K0, Ckdk0),$$

and decrypts the encrypted data Cmkd by the decrypted crypt key Kd

$$M=D(Kd, Cmkd).$$

Summary of the Invention

The present invention provides a concrete structure for applying the invention of the crypt key system described in the previous applications to the television system, the database system or the electronic commercial transaction system or the like.

This system comprises a broadcasting station, a database, a receiving apparatus, a data communication apparatus, and a user terminal. As the crypt key system, secret-key cryptosystem and the public-key cryptosystem are used. In addition, the digital signature is used, and the crypt key is supplied through broadcasting with either encrypted or uncrypted.

The present invention is effective in the prevention from unjustified use or the copyright management in the database system, a pay-per-view system, or a video-on-demand system. Furthermore, the present invention is a useful means in the realization of an electronic market using the electronic data interchange system.

Brief Description of the Drawings

Fig. 1 is a structural view of a crypt key system according to the prior applications.

Fig. 2 is a structural view of the crypt key system according to a first embodiment of the present invention.

Fig. 3 is a structural view of the crypt key system according to a second embodiment of the present invention.

Fig. 4 is a structural view of the crypt key system according to third and fourth embodiments of the present invention.

Figs. 5(a), 5(b) and 5(c) are structural views of fifth embodiment to which the present invention is applied.

Embodiments

Embodiments of the present invention will be described by using Figs. 2 through 4.

[Embodiment 1]

A system shown in Fig. 2 is a crypt key system of the embodiment 1 in which the present invention is applied to a database system. This system comprises a broadcasting station 11 which either a multiplex broadcasting by of BS, CS, a terrestrial wave television, or FM broadcasting or the like, or data broadcasting by a digital broadcasting, a database 12 in which various kinds of data including moving picture data is stored, a charging center 13, a receiving apparatus 14 for receiving the data broadcasting offered by the broadcasting station 11, a data communication apparatus 15 for communicating with the database 12 and the user terminal 18 for using the data.

The database 12 and the broadcasting station 11, and the database 12 and the charging center 13 are connected with a direct means connecting with a communication line such as a dedicated line or an indirect means such as a flexible disc or the like. The database 12 and the data communication apparatus 5 are connected with a communication line 17 such as a communication line, or CATV line or the like. Then, the broadcasting station 11 and the receiving apparatus 14 are connected with a radio wave 16 such as a terrestrial wave television broadcasting, satellite television broadcasting, CATV broadcasting, FM broadcasting or a satellite data broadcasting or the like. The receiving apparatus 14 and the user terminal 18, and the data communication apparatus 15 and the user terminal 18 are connected with a direct means such as a connection cable or an indirect means such as a flexible disc or the like.

What is shown with a solid line in Fig. 2 is an uncrypted data path and what is shown with a broken line is an encrypted data path.

Incidentally, data exchange between the database 12 and the broadcasting station 11, and the database 12 and the charging center 13 are, in principle, carried out with a dedicated line or a flexible disc. In addition, a public line, a broadcasting satellite, a communication satellite or a terrestrial wave broadcasting can be used. In such a case, the data is encrypted.

In this system, the secret-key cryptosystem and the public-key cryptosystem are used.

The database 12 prepares the public-key Kbd and the private-key Kvd to supply the public-key Kbd to the broadcasting station 11. The broadcasting station 11 which receives the public-key Kbd broadcasts it by a teletext multiplexing broadcasting using scanning lines during the retrace blanking interval period of an arnalog television picture signal, the data broadcasting using a sub audio band of the analog television audio signal, FM multiplex data broadcasting or digital data broadcasting.

Further, in this case, a digital signature of the database 11 can be done to the public-key Kbd.

The data may be supplied without encrypting the menu in which the titles of data which can be used, the content introduction of the data, product catalogs, order forms, blank checks, the copyright information for the convenience of the data usage.

The receiving apparatus 14 which receives the transferred public-key Kbd sends the public-key Kbd to the user terminal 18. The user terminal 18 which receives the transferred public-key Kbd stores the public key Kbd in the recording medium such as a semiconductor memory, a flexible disc, or a hard disc or the like.

Users who select the data which they request for usage by means of menu or the introduction of contents request for the use of data M to the database 12 via a communication line 17 by the data communication apparatus 15.

At this time, the user encrypts the public-key Kbd of the database 12 by own secret-key Ksu which has received from the database 12

$$Cksukbd=E\ (Kbd,\ Mksu)$$

and transmits it to the database 12.

The database 12 decrypts the encrypted secret-key Cksukbd of the user by the private-key Kvd

$$Ksu=D\ (Kvd,\ Cksukbd)$$

and encrypts the data M which is requested for use by the decrypted user secret-key Ksu

$$Cmksu=E\ (Ksu,\ M),$$

and transmits it to the data communication apparatus 15 of the user via the communication line 17.

The user who receives the data Cmksu encrypted by own secret-key Ksu decrypts the encrypted data Cmksu with the user terminal 18

$$M=D\ (Ksu,\ Cmksu)$$

to use it.

This system is provided with charging center 13 which is incorporated with the database 12. This charging center 13 is used when the data is provided with pay basis. In the case where the data is one which is provided with free such as shopping information or the like, this charging center 13 is not used. However, even the data provided with free such as shopping information or the like, the charging center is used in the case where charges are to be settled along with orders.

[Embodiment 2]

Fig. 3 shows a crypt key system according to embodiment 2 in which the present invention is applied to a video on demand (VOD) system which broadcasts television programs corresponding to the requests from users.

This system comprises a CATV station 21, a charging center 23, a receiving apparatus 24, a data communication apparatus 25 and a user terminal 28.

The charging center 23 is used when the television program is provided on pay basis but not used when the television program is provided without charges along with advertisement.

In this system, the encrypted television broadcast programs and the crypt key are transmitted with the CATV line 27 which is a single path.

The CATV station 21 and the charging center 23 are connected with a direct means for electrical connection with a communication line such as a dedicated line or the like, or an indirect means such as flexible disc or the like. The CATV station 21 and the receiving apparatus 24, the CATV station 21 and the data communication apparatus 25 are connected with the CATV cable 27. The receiving apparatus 24 and the user terminal 28, the data communication apparatus 25 and the user terminal 28 are connected with a direct means such as a connection cable or an indirect means such as a flexible disc or the like.

What is shown with a solid line in Fig. 3 is an uncrypted data path and what is shown with a broken line is an encrypted data path.

Incidentally, the data exchange between the CATV station 21 and the charging center 23 is carried out through a dedicated line or a flexible disc in principle. Additionally, the data exchange is also carried out by means of the communication line or the broadcasting satellite, the communication satellite and the terrestrial wave broadcasting. In this case, the data is encrypted.

In this system, the CATV system is treated as one kind of database. As a crypt key method, the secret-key cryptosystem and the public- key cryptosystem are adopted.

Users who use this VOD system either registers their own public-key Kbu with the CATV station 21 in advance, or transmit the public-key Kbu by using the communication apparatus 25 at the time when the request for usage.

The CATV station 21 encrypts the secret- key Ksb of the CATV station 21 by the transmitted public- key Kbu of users

$$Cksbkbu=E\ (Kbu,\ Ksb)$$

and transmits it to the data communication apparatus 25 via the CATV line 27

The television program M is encrypted by using the secret-key Ksb of the CATV station 21

$$Cmksb=E\ (Ksb,\ M)$$

and is broadcast to the receiving apparatus 24 via the CATV line 27.

The user decrypts the received encrypted secret-key Cksbkbu of the CATV station 21 by the private-key Kvu of user

Ksb=D (Kvu, Cksbkbu)

and decrypts the encrypted television program Cmksb using the decrypted secret-key Ksb of the decrypted CATV station 21

M=D (Ksb, Cmksb)

for use.

In addition, this crypt key system is applicable, if encryption is available, to the television broadcasting other than CATV, audio broadcasting, or data broadcasting. As a method for transmitting the crypt key from the broadcasting station, the teletext multiplex broadcasting using the scanning lines during the retrace blanking inverval of an analog television ppicture signal, the data broadcasting using an sub audio band of the analog television audio signal, FM multiplex data broadcasting, or digital data broadcasting can be also used.

In addition, this crypt key system can be used when the crypt key is distributed in the data copyright management system which is described in prior Japanese Patent Applications Nos. 6-64889, 6-237673, 6-264199, 6-264201 and 6-269959 proposed by the present inventor.

This crypt key system can be also applied to a case where a recording medium such as a CD-ROM or the like in which a plurality of informations are encypted with a plurality of different patterns and are recorded, which is described in Japanese Laid-Open Patent Application No. 6-132916, proposed by the present inventor.

These inventions of previous applications are explained hereinbelow.

An outline of the data copyright management system described in Japanese Patent Application No. 6-64889 is described as follows.

To control the copyright in the display (including the process to sound), storage, copy, edit and transfer of digital data in the database system including a real time transmission of a digital picture, any one or a plurality among a program for managing the copyrights a copyright information and a copyright management message are transmitted, when needed, in addition to a permit key for allowing the use of encrypted data corresponding to usage requests from users.

The copyright management message is displayed on a screen and advises or warns to the user in case the data is utilized other than the conditions of user's request or the permission. T the copyright management program watches and controls in order that the data is not utilized beyond the conditions of user's request or the permission.

The copyright management program, the copyright information and the copyright management message are supplied together with a permit key in some cases, or they are supplied together with data in some other cases. Or, a part of them is supplied together with the permit key, and other part is supplied with the data.

For data, the permit key, the copyright management message, the copyright information and the copyright management program, there are the following three cases: a case where these are transmitted with encrypted, and upon using, the encryption is decrypted, a case where they are transmitted with encrypted and remain in encrypted except being decrypted only when they are displayed, and a case where they are not encypted at all.

An outline of the data copyright management system described in Japanese Patent Application No. 6-237673 is described as follows.

This database copyright management system comprises a database in which uncrypted data is stored, a data supply means of a broadcasting station such as satellite broadcasting station for broadcasting the encrypted data from the database, or of a recording medium such as a CD-ROM where encrypted data from the database is recorded, a communication network, a key control center for controlling a crypt key, and a copyright management center for controlling copyrights of the database. Then, the database utilization program for using the database, the copyright management program for controlling the copyrights, a first crypt key and a second crypt key are used.

A first user registers with the key control center in advance for using the database. At that time, the database use program is distributed. This database utilization program includes information on the first user and a program for generating a crypt key unique to the first user with a predetermined algorithm by using the information.

The data is stored in the database without encrypted, and when it is distributed by broadcast, or through recorded on a recording medium or a communication network, the data is encrypted by the first crypt key to an encrypted data.

The encrypted data is stored in recording medium such as a semiconductor memory of the first user terminal, a flexible disc or hard disc, when distributed via broadcasting or communication network, is stayed as is when recorded in a CD-ROM recording medium and distributed, or is stored in the recording medium such as a semiconductor memory of the first user terminal, a flexible disc or a hard disc or the like.

The first user who uses the data directly from the database requests a key for decrypting and using the encrypted data to the key control center via the communication network. Information concerning the first user is presented at this time.

The key control center transfers the information on the first user to the copyright management center while the copyright management center uses information I concerning the first user to generate a crypt key peculiar to the first user by a predetermined algorithm, and the generated first user crypt key is used to encrypt the copyright management program, the first crypt key and the

second crypt key to be transferred to the key control center.

The copyright management program encrypted by using the crypt key generated by using the information on the first user is peculiar to the first user.

The key control center which receives the encrypted copyright management program transmits to the first user terminal each of the encrypted copyright management program, the first crypt key and the second crypt key via the communication network. Then, the first user stores the received encrypted copyright management program, the first crypt key and second crypt key in a recording medium such as a semiconductor memory, a flexible disc, or a hard disc.

The first user generates the crypt key peculiar to the first user by using a database utilization program which is distributed in advance and using information on the first user with a predetermined algorithm. Then, the first user decrypts the encrypted copyright management program, the encrypted first and second crypt keys, and the encrypted data is decrypted by the decrypted first crypt key.

In the case of storing, copying and transferring the decrypted data, it is encrypted by the second crypt key decrypted with the decrypted copyright management program. Then, the encrypted data is stored in the recording medium such as the semiconductor memory of the first user terminal, the flexible disc or the hard disc or the like. When the first user uses the stored encrypted data, it is decrypted by using the second crypt key. Then, this operation is repeated for primary sue of the data.

When the encrypted data is copied on the external memory medium or is transferred to the second user terminal via the communication network, the first crypt key and the second crypt key are disued by the copyright management program. The first user then,cannot use the encrypted data.

At this time, when the encrypted data is stored in the first user terminal, information on the first user

user who has received the copy or the transfer of the encrypted data from the first user. Thus, the request for the secondary use is not accepted.

The copyright management center which acepts the request of the secondary use transmits the second crypt key for decrypting the encrypted data, the third crypt key for reencrypting and redecrypting the decrypted data and the copyright management program for the aforementioned decryption, the reencryption and redecryption, to the second user.

The outline of the copyright management system described in the Japanese Patent Application No. 6-264199 is described as follows.

This copyright management system uses the first public-key prepared by the user,
the first private-key corresponding to the first public-key, the second public-key, the second private-key corresponding to the second public-key, and the first secret-key and the second secret-key prepared by the database.

The database side encrypts the data which is not encrypted by using the first secret-key, and encrypts the first secret-key by the first public-key, and the second secret-key by the second public-key. These encrypted data and the encrypted first secret-key and second secret-key are transmitted to users.

The user decrypts the encrypted first secret-key by using the first private-key and decrypts the encrypted data by the decrypted first secret-key for use. Then, the user decrypts the encrypted second secret-key by the second private-key so that the decrypted second secret-key is used as a crypt key for data storage, copy and transfer after the decryption of the data.

The outline of the data copyright management system described in the Japanese Patent Application No. 6-264201 is described as follows.

In the case where new data is prroduced by editing a plurality of encrypted data which are obtained from the database and is accepted to be supplied to others, the